BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 10208386
PUBLICATION DATE : 07-08-98

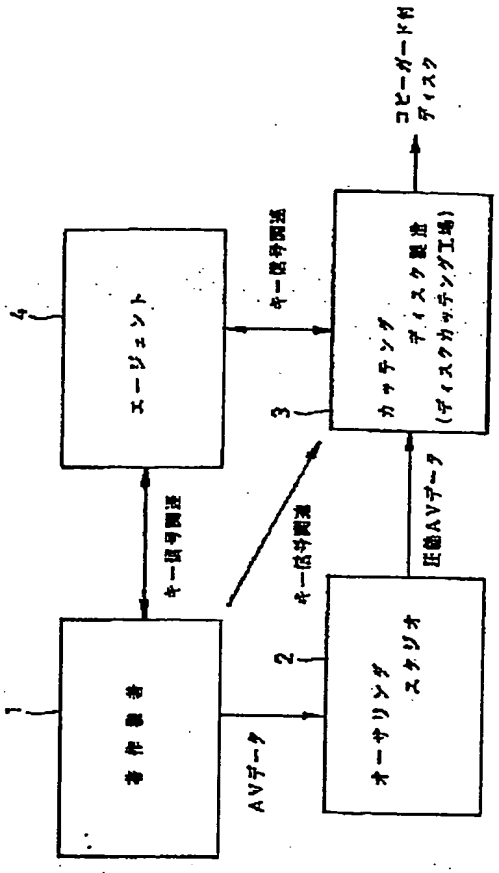
APPLICATION DATE : 27-01-97
APPLICATION NUMBER : 09012674

APPLICANT : SONY CORP;

INVENTOR : SHINKAI YOTARO;

INT.CL. : G11B 20/10 G11B 7/24 G11B 7/26 H04L 9/14

TITLE : RECORDING MEDIUM AND DISK CUTTING DEVICE



ABSTRACT : PROBLEM TO BE SOLVED: To make a third person impossible to obtain a key signal directly from the recording medium, by recording a scrambled signal, a cryptographic key signal produced by moreover ciphering a key signal generated based on random numbers and ciphered section control information for controlling a ciphered section of scramble and key signals.

SOLUTION: AV data as an original data belonging to a copyright holder 1 is compressed and multiplexed in an authoring studio 2, and is ciphered in a disk cutting factory 2 by a key signal in relation to such a key signal under management by a key signal management agent 4, and then a disk is cut. Then, at the time of manufacturing a cutting data in the disk cutting factory 3, the data is scrambled by a key signal for encipherment. Particularly, an operating section is controlled so as to change the key signal depending only upon the inside with regard to time intervals.

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平１０－２０８３８６

(43)公開日　平成10年(1998)8月7日

(51)Int. Cl.[6]		識別記号	FI		
G１１B	20/10		G１１B	20/10	H
	7/24	５２２		7/24	５２２　Z
	7/26			7/26	
H０４L	9/14		H０４L	9/00	６４１

審査請求　未請求　請求項の数２　ＯＬ　（全１５頁）

(21)出願番号　特願平9-12674

(22)出願日　平成9年(1997)1月27日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川6丁目7番35号

(72)発明者　新海　陽太郎
東京都品川区北品川6丁目7番35号　ソニー株式会社内

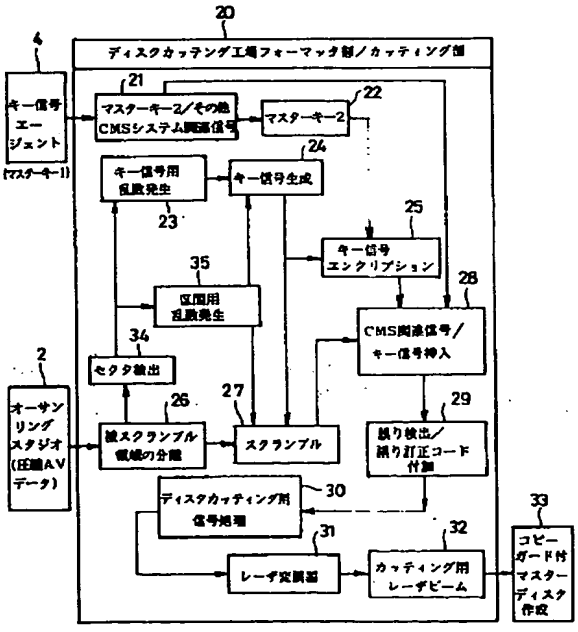
(74)代理人　弁理士　松隈　秀盛

(54)【発明の名称】記録媒体およびディスクカッティング装置

(57)【要約】

【課題】　オリジナル信号を記録したディスクを第三者が再生しても不正コピーができない記録媒体およびディスクカッティング装置の提供を目的とする。

【解決手段】　ディスクカッティング装置は、入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成するキー信号用乱数発生部２３と、キー信号に基づいて入力信号に対してスクランブルをかけるスクランブル部２７と、乱数に基づいて発生させたキー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に入力信号のスクランブルおよびキー信号の暗号化を行う区間を制御する暗号化区間制御情報とをスクランブルをかけられた被スクランブル信号に挿入するＣＭＳ関連信号／キー信号挿入部２８とを備え、これらのデータからカッティングデータを生成して、マスターディスク３３を作成するようにした。



本実施の形態のディスクカッティング工場のフォーマッタ部とカッティング部の構成を示す図

1

【特許請求の範囲】

【請求項１】　複数の素材信号がそれぞれ符号化され、符号化された複数の素材信号が多重化されてオリジナル信号が新規に作成されたとき、上記オリジナル信号が所定のキー信号に基づいてスクランブルされた被スクランブル信号と、

乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号と、

特定の区間または任意の区間毎に上記オリジナル信号のスクランブルおよび上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報と、

を記録するようにしたことを特徴とする記録媒体。

【請求項２】　入力信号から、上記入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成するキー信号生成手段と、

上記キー信号に基づいて上記入力信号に対してスクランブルをかけるスクランブル手段と、

乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを、上記スクランブル手段によりスクランブルをかけられた被スクランブル信号に挿入する挿入手段と、

を備え、上記挿入手段により上記暗号化キー信号および上記暗号化区間制御情報とを上記被スクランブル信号に挿入したデータからカッティングデータを生成して、上記カッティングデータに基づいてマスターディスクを作成するようにしたことを特徴とするディスクカッティング装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば、ＤＶＤ（ディジタル・ビデオ・ディスク）に記録すべきデータを記録した記録媒体およびこのデータに基づいてマスターディスクを作成するディスクカッティング装置に関する。

【０００２】

【従来の技術】図４に、ビデオデータとオーディオデータとを同時に符号化処理するエンコーダを用いたＤＶＤの編集システム（オーサリングシステム）の構成例を示す。このオーサリングシステムは、ディジタルＶＴＲ４０と、エンコーダ４１と、コンピュータ４２とを有する。

【０００３】このディジタルＶＴＲ４０は、ディジタル方式で記録されたビデオテープＴＰ（Ｔａｐｅ１）からディジタルビデオデータを再生するビデオ再生部４０Ａと、ディジタル方式で記録されたオーディオテープＴＰ（Ｔａｐｅ２）からディジタルオーディオデータを再生するオーディオ再生部４０Ｂとを有する。

【０００４】エンコーダ４１は、コンピュータ４２による制御によってディジタルＶＴＲ４０から再生されるビデオデータＤｖおよびオーディオデータＤａをそれぞれ符号化し、さらにこれら符号化されたビデオデータおよび符号化されたオーディオデータとを多重化して一連のビットストリームとして出力する。

【０００５】ビデオデータＤｖおよびオーディオデータＤａの各符号化は、ＭＰＥＧ２（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ２）によるデータ圧縮のための符号化であり、コンピュータ４２の主記憶装置にストアされたビデオ符号化プログラムおよびオーディオ符号化プログラムにそれぞれ記述された各アルゴリズムに従って行われ、符号化されたビデオデータと符号化されたオーディオデータの多重化は、同じくコンピュータ４２の主記憶装置にストアされた多重化プログラムに記述されたアルゴリズムに従って行われる。

【０００６】このようにして、このオーサリングシステムにおいては、ディジタルＶＴＲ４０等からの再生データとしてのビデオデータＤｖおよびオーディオデータＤａを符号化処理し、ビデオデータＤｖおよびオーディオデータＤａとをそれぞれ所定のデータレートに変換する。

【０００７】このようなオーサリングシステムでのデータの作成はスタジオ等で行われ、オーサリングシステムで作成したデータを記録媒体に記録して、カッティングマシーンのある工場に持ち込んで、両者を予め決められたフォーマットに並び変えて、ＤＶＤなどの記録媒体に記録することにより、マスターディスクを製作するようにしていた。

【０００８】

【発明が解決しようとする課題】しかし、従来のオーサリングシステムおよびカッティングマシーンにより、真正な製作者が製作した正規な信号データを記録したディスク等の記録媒体から、第三者が信号データを再生させて、この再生データを記録媒体にコピーして不正なデータを作るようなことがあった場合でも、このような不正なデータによるコピーを防止することができないという不都合があった。

【０００９】これに対して、従来では、以下に述べる２つのコピー対策は講じられていた。第１のコピー対策は、カッティングマシーンにおけるカッティング中に信号部分のある特定のビット（例えばＬＳＢ）を反転させて信号部分にカッティング時の痕跡を残すようにして、このカッティング時の痕跡を検出することにより、扱う信号がコピーしたものであるのか、オリジナルなものであるのかを判定するものである。なお、この特定のビットの反転は、人間には判別できない程度のものであり、画像上でも影響の無いものであり、信号がコピーかオリジナルかの判定のみに用いられる。しかし、この特定のビットは後からオリジナルデータに対して追加されるものであり、このような判定も特定ビットの反転を検出す

2

ることができる再生装置でのみできるので、通常のプレーヤー等で何等問題なく信号を再生することができるため、コピーの対策としては不十分である。

【００１０】また、第２のコピー対策は、ＤＡＴ（ディジタルオーディオテープ）システム等で採用されているＳＣＭＳ（シングルコピーマネージメントシステム）方式によるコピー制限であり、ディジタルコピー禁止ビットのフラグを１回だけ立てることにより、１回だけコピーを許可するものである。しかし、このような方式でも１回だけならコピーができるので、同様に、コピーの対策としては不十分である。

【００１１】このように両者とも対策後のデータと非対策データとを比較したり、非コピーガード時とコピーガード時とのコントロールビットのビット配置を比較したりすることで、比較的容易にコピー防止をするための手段を読み取られてしまい、それを利用してコピー防止の効果を無効にしてしまう手段が出現していた。従って、データ内容を読み取られても一義的にはコピー防止すべき手段が分からないコピー防止方法が望まれていた。

【００１２】本発明は、かかる点を考慮してなされたものであり、オリジナル信号を記録したディスクを再生しても再生データのコピーができない記録媒体およびディスクカッティング装置の提供を目的とする。

【００１３】

【課題を解決するための手段】本発明の記録媒体は、複数の素材信号がそれぞれ符号化され、符号化された複数の素材信号が多重化されてオリジナル信号が新規に作成されたとき、上記オリジナル信号が所定のキー信号に基づいてスクランブルされた被スクランブル信号と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号と、特定の区間または任意の区間毎に上記オリジナル信号のスクランブルおよび上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報と、を記録するようにしたものである。

【００１４】また、本発明のディスクカッティング装置は、入力信号から、上記入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成するキー信号生成手段と、上記キー信号に基づいて上記入力信号に対してスクランブルをかけるスクランブル手段と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを、上記スクランブル手段によりスクランブルをかけられた被スクランブル信号に挿入する挿入手段と、を備え、上記挿入手段により上記暗号化キー信号および上記暗号化区間制御情報とを上記被スクランブル信号に挿入したデータからカッティングデータを生成して、上記カッティングデータに基づいてマスターディスクを作成するようにしたものである。

【００１５】また、本発明の記録媒体およびディスクカッティング装置によれば、以下の作用をする。本発明の記録媒体は、上記オリジナル信号が所定のキー信号に基づいてスクランブルされた被スクランブル信号と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号と、特定の区間または任意の区間毎に上記オリジナル信号のスクランブルおよび上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報と、を記録するようにしたので、キー信号が直接的に外部に出ることがなくなると共にキー信号の暗号化を複雑にし、キー信号の盗用を防止することができ、これにより、第三者による不正コピーを防止することができる。

【００１６】また、本発明のディスクカッティング装置において、キー信号生成手段は入力信号から上記入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成し、スクランブル手段は上記キー信号に基づいて上記入力信号に対してスクランブルをかけ、挿入手段は乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを上記スクランブル手段によりスクランブルをかけられた被スクランブル信号に挿入し、上記挿入手段により上記暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを上記被スクランブル信号に挿入したデータからカッティングデータを生成して、上記カッティングデータに基づいてマスターディスクを作成するように作用する。

【００１７】

【発明の実施の形態】以下、本実施の形態について説明する。本実施の形態は、例えばＤＶＤなどのパッケージメディアに記録されているデータを第三者が再生装置で再生し、再生データ列をあたかもオリジナルデータのごとくコピーして再利用する不正コピー防止のために、記録されている元のデータ列をキー信号により予め区間を制御してスクランブルをかけて暗号化し、そのまま第三者がコピーしたのではそのデータ列が再利用できなくなるようにしたものである。特に、暗号化キー信号及びキー信号の暗号化に関する区間を制御する情報等の秘密を護るため、その受け渡しや管理が重要となるが、この実施の形態は、その機密保持を効果的に行うものである。

【００１８】本実施の形態では、このようなコピー防止対策において、元のデータ列を暗号化する、例えばディスクカッティング工場において、受け渡しされたデータ列に対してキー信号に従って区間を制御してスクランブルをかけ、それ以後必要な変調等を行ってマスターディスクのカッティング等を経てパッケージメディアを作成する。ここで、この暗号化に必要なキー信号およびキー信号の暗号化を行う区間を制御する情報を外部より人間

等を介して受け渡しするのではなく、暗号化を行う、例えばディスクカッティング工場ではフォーマッタ部において自動生成されるものであり、これによりキー信号が外部に流出することがなくなり、キー信号の機密が一層護られ、キー信号の盗用に強くすることでコピー防止を行うものである。

【００１９】このように、ＤＶＤ等のパッケージメディアにおいては、その再生データが第三者によりコピーされて別に利用されていることがあり、データ供給者はこれにより損害を被るためコピー防止対策が必要になっている。またその際、第三者側で容易にコピー防止の対策がとれないようにすることも必要であり、本実施の形態の前提として、ＤＶＤではデータを読んでも一義的に解読できないようにするため、コピー防止にＣＭＳ（Ｃｏｐｙｒｉｇｈｔ　Ｍａｎｅｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）という手法を用いて元のデータを暗号化しているが、これはキー信号で、データにスクランブルをかけて、かつそのキー信号も一義的に解読できないように別の手段でエンクリプト（暗号化）してからデータ列に挿入している。

【００２０】本実施の形態は、このようなＣＭＳによるコピー防止において、記録データを正規の信号に再生する際に必要なキー信号をディスクカッティング工場のフォーマッタ部の外部に出さないようにしてクローズドループの中で処理することにより、より高度な機密性をもたらし、コピー防止をより完全に近づけるものである。

【００２１】まず、図１を参照しながら、本実施の形態のＣＭＳにおけるコピー防止システムの概要を説明する。このＣＭＳにおけるコピー防止システムは、オリジナルデータとしてのＡＶ（オーディオ・ビデオ）データを製作する著作権者１と、ＡＶデータを圧縮して多重化するオーサリングスタジオ２と、キー信号に関連した各種暗号化関連信号を管理するキー信号管理エージェント４と、圧縮ＡＶデータをキー信号関連信号により暗号化してからディスクをカッティングするカッティングディスク製造部（ディスクカッティング工場）３とを有する。

【００２２】このように構成された、このＣＭＳにおけるコピー防止システムは、以下のように動作する。このシステムは、著作権者１のＡＶデータでＤＶＤ等のパッケージメディアをつくる際に使用されるものであり、著作権者１が所有するオリジナルデータとしてのＡＶデータを、オーサリングスタジオ２において圧縮して多重化し、キー信号管理エージェント４により管理されていたキー信号に関連した信号により、ディスクカッティング工場３において暗号化してからディスクをカッティングするようにした。

【００２３】このように、ディスクに記録されたデータを第三者が再生して、オリジナルデータを不正にコピーされても再利用できないようにして、ディスクカッティング工場３においてカッティングデータ作成時に暗号化のためにキー信号でスクランブルをかけるようにする。ここで、特に、本実施の形態では、暗号化に用いたキー信号を外部に出さないようにすると共に、キー信号が内部のみに依存して時間間隔に関して変化するように動作区間が制御されるようにしている。

【００２４】上述したオーサリングスタジオ２は、例えば、エンコードおよびマルチプレクス部と、オーサリングデータ生成部と、信号データ出力回路とを有する。エンコードおよびマルチプレクス部は信号データ入力部から供給される複数の素材となる信号データを圧縮処理するために符号化を行うと共に符号化された複数の素材となる信号データを多重化して、オリジナルの信号データを出力する機能を有する。

【００２５】オーサリングデータ生成部は、キー信号を挿入すると共に、所定のサイズにセクタライズしてオーサリングデータを生成する機能を有する。

【００２６】信号データ出力回路は、オーサリングデータ生成部から供給される信号データを所定の記録媒体に記録して出力する機能を有する。信号データ出力回路は、ディスク出力部と、テープ出力部と、ハードディスク出力部と、オンラインデータ出力部とを有する。ディスク出力部と、テープ出力部と、ハードディスク出力部と、オンラインデータ出力部は、各出力信号の記録される媒体の形式によって切り換えられる。ディスク出力部は記録媒体がディスクの場合に用いられ、ディスク記録装置で構成される。テープ出力部は記録媒体がテープの場合に用いられ、テープ記録装置で構成される。ハードディスク出力部は記録媒体がハードディスクの場合に用いられ、ハードディスク装置で構成される。また、オンラインデータ出力部は転送の媒体がオンラインデータの場合に用いられ、オンラインケーブルで構成される。

【００２７】また、エージェント４は、キー信号関連信号の管理手段としての機能を有し、キー信号関連信号生成部と、キー信号関連信号出力部とを有する。また、キー信号関連信号出力部は、例えばフロッピーディスク出力部と、キーボード出力部等を有する。

【００２８】上述したディスクカッティング工場３は、フォーマッタ部とカッティング部とを有する。本実施の形態のフォーマッタ部１０は、図２に示すように、エージェント４から供給されるキー関連信号とは別にフォーマッタ内部で発生させるキー信号によりオーサリングスタジオ２から供給されるＡＶデータに暗号化区間制御情報に基づいてスクランブルをかけるキー信号によるスクランブル部１１と、キー信号をキー信号の暗号化区間制御情報に基づいてエンクリプションをかけて被スクランブルデータにエンクリプトされたキー信号およびキー信号の暗号化区間制御情報を挿入するエンクリプテドキー信号挿入部１２と、エンクリプテドキー信号およびキー信号の暗号化区間制御情報が挿入された被スクランブル

データをディスク記録用に信号変換するフォーマッタによる信号変換部１３とを有する。

【００２９】このように構成されたディスクカッティング工場のフォーマッタ部１０は、以下のような動作をする。エージェント４のキー信号関連信号出力部から例えばフロッピーディスクやキーボードや通信等の様々な形態でキー信号関連信号がディスクカッティング工場のフォーマッタ部１０のキー信号によるスクランブル部１１に供給される。また、オーサリングスタジオ２から圧縮ＡＶデータがディスクカッティング工場のフォーマッタ部１０のキー信号によるスクランブル部１１に供給される。フォーマッタ部１０のキー信号によるスクランブル部１１において、暗号化区間制御情報に基づいてスクランブルをかけるキー信号を発生させ、このキー信号を用いて圧縮ＡＶデータのデータ列の信号部分に区間を制御してスクランブルをかける。被スクランブル信号はエンクリプテドキー信号挿入部１２に供給される。エンクリプテドキー信号挿入部１２においてキー信号が暗号化区間制御情報に基づいてエンクリプト（暗号化）され、エンクリプトされたキー信号およびキー信号暗号化区間制御情報が被スクランブルデータに挿入される。エンクリプテドキー信号およびキー信号暗号化区間制御情報が挿入された被スクランブルデータはフォーマッタによる信号変換部１３に供給される。フォーマッタによる信号変換部１３においてエンクリプテドキー信号およびキー信号暗号化区間制御情報が挿入された被スクランブルデータはディスク記録用に信号処理される。

【００３０】このようにして、キー信号をフォーマッタ内部で生成するので、キー信号を媒体を介せずに発生させることができ、エンクリプションされないキー信号自体が決して外部に出ることはなく、さらにキー信号暗号化区間制御情報によりキー信号が内部にのみ依存して時間間隔に関しても変化するように動作区間が制御されるので、キー信号の暗号化が複雑になり、第三者がディスク記録媒体からキー信号を盗むことができず、従ってＣＭＳを用いたコピー防止機能を有効に発揮させることができる。

【００３１】上述したディスクカッティング工場は、フォーマッタ部とカッティング部とを有する。図３に本実施の形態のディスクカッティング工場のフォーマッタ部とカッティング部２０の構成を示す。このフォーマッタ部はエージェントから供給されるキー信号関連信号からフォーマッタ部内部で生成し、エージェントが所有するマスターキー１でエンクリプトされたスクランブル用キー信号（＝タイトルキー）をエンクリプションするマスターキー２と生のマスターキー２（＝ディスクキー）とＰＣ間の検査用のＡＣコードなどのその他ＣＭＳシステム関連信号を検出するマスターキー２／その他ＣＭＳシステム関連信号検出部２１と、それらのＣＭＳシステム関連信号から生のマスターキー２を検出して取り出すマスターキー２検出部２２と、キー信号用の乱数を発生させるキー信号用乱数発生部２３と、キー信号用乱数および区間用乱数に基づいてキー信号を生成するキー信号生成部２４と、オーサリングスタジオ２から供給される圧縮ＡＶデータからスクランブルされるべき領域を分離する被スクランブル領域分離部２６と、スクランブルされるべき領域の圧縮ＡＶデータに対してフォーマッタ部内部で乱数に基づいて生成されたキー信号によりスクランブルを行うスクランブル部２７とを有する。上述した部分が、図２に示したキー信号によるスクランブル部１１に対応する。

【００３２】また、このフォーマッタ部は、圧縮ＡＶデータから区間用乱数発生区間のセクターを検出するセクター検出部３４と、キー信号を用いてキー信号の暗号化区間制御情報に基づいてスクランブルされるべき領域の圧縮ＡＶデータにスクランブルをかけると共にキー信号にエンクリプションをかけるようにキー信号暗号化区間制御情報としての区間用乱数を発生させる区間用乱数発生部３５と、フォーマッタ部内部でキー信号用乱数および区間用乱数に基づいて生成されたキー信号をマスターキー２を用いてエンクリプションするキー信号エンクリプション部２５と、スクランブルされた圧縮ＡＶデータにエンクリプションされたマスターキー２及び同じくエンクリプトされたキー信号、暗号化区間制御情報およびその他ＣＭＳシステム関連信号を挿入するＣＭＳ関連信号／キー信号挿入部２８とを有する。上述した部分が、図２に示したエンクリプテドキー信号挿入部１２に対応する。

【００３３】また、このフォーマッタ部は、誤り検出コード（ＥＤＣ）を付加し、誤り訂正コード（ＥＣＣ）処理をする誤り検出／誤り訂正コード付加部２９と、ディスクに記録する信号に適した８／１６変調や、付加情報を含む同期信号を信号ブロックの先頭に挿入する同期挿入等の処理を行うディスクカッティング用信号処理部３０とを有する。上述した部分が、図２に示したフォーマッタによる信号変換部１３に対応する。

【００３４】また、カッティング部は、８／１６変調や同期挿入等の処理を施したデータにレーザ変調を施すレーザ変調器３１と、レーザ変調されたデータに応じてレーザビームを発生させて、マスターディスクをカッティングしてコピーガード付マスターディスク３３を作成するカッティング用レーザービーム発生部３２とを有する。

【００３５】次に、図１に示したオーサリングスタジオおよびディスクカッティング工場の詳細な構成を図２および図３を用いて説明する。まず、オーサリングスタジオ２について説明する。エンコードおよびマルチプレクス回路は、映像信号を符号化するエンコード回路と、音声信号を符号化するエンコード回路と、補助データ信号を符号化するエンコード回路と、符号化された音声信号

と音声信号および補助データ信号をそれぞれ多重化するマルチプレクス回路とを有する。エンコード回路、エンコード回路およびエンコード回路は、ＭＰＥＧ２（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔｓ　Ｇｒｏｕｐ２）によるデータ圧縮のための符号化を行う。ＭＰＥＧ標準には、ＣＤ－ＲＯＭ等の蓄積メディアのための圧縮符号化標準であるＭＰＥＧ１と、ＭＰＥＧ１のアプリケーションも含む広い範囲のアプリケーションのための圧縮符号化標準であるＭＰＥＧ２とがあるが、本実施の形態ではＤＶＤの動画圧縮に最適なＭＰＥＧ２を用いている。

【００３６】映像用のエンコード回路は、ＭＰＥＧ２による動画圧縮を行うように、入力信号をＤＣＴ（Ｄｉｓｃｒｅｔｅ　Ｃｏｓｉｎｅ　Ｔｒａｎｓｆｏｒｍ）変換するＤＣＴ変換回路と、ＤＣＴ変換された係数を量子化する量子化回路と、量子化された変換係数を逆量子化する逆量子化回路と、逆量子化された変換係数を逆ＤＣＴ変換する逆ＤＣＴ変換回路と、逆ＤＣＴ変換された信号に動き補償をする動き補償回路と、動き補償された信号を逆ＤＣＴ変換された信号に加算する加算器と、入力信号から動き補償された信号を減算する減算器とを有する。

【００３７】音声用のエンコード回路は、入力信号の時間サンプルを周波数成分のサブバンドに変換するフィルタバンクと、入力信号を聴覚心理モデルによりビット割り当てするビット割当回路と、この周波数成分のサブバンドをサブバンド毎に量子化する量子化回路と、ビットストリーム形成回路とを有する。

【００３８】マルチプレクス回路は、エンコード回路、エンコード回路およびエンコード回路で符号化された映像、音声および補助データのビットストリームを同期を含めて統合して１本化するようにして多重化する。この多重化の方式には、１つのプログラム（番組）を構成するプログラム・ストリーム（Ｐｒｏｇｒａｍ　ｓｔｒｅａｍ，ＭＰＥＧ２－ＰＳ）と、複数のプログラムを同時に構成できるトランスポート・ストリーム（ｔｒａｎｓｐｏｒｔ　ｓｔｒｅａｍ，ＭＰＥＧ２－ＴＳ）の２種類の方式がある。本実施の形態では、ＭＰＥＧ２－ＰＳを用いている。このようにして、メインの信号データのビットストリームが生成されるように構成される。

【００３９】パケットによる多重化は、例えば、映像、音声、補助データ等の信号データを多重化する場合、映像、音声、補助データ等のそれぞれをパケットと呼ばれる適当な長さのストリーム（ビット列）に分割して、後述するヘッダ信号等の付加情報を付加して、適宜、映像、音声、補助データ等のデータのパケットに切り換えて時分割して一本のビットストリームにする。これらの各パケットには、先頭部分に後述するヘッダ信号と称される映像、音声、補助データ等のデータの属性を識別する情報が設けられる。

【００４０】パケット長は、蓄積メディアまたは伝送ネットワークの仕様に依存する。例えば、光ディスクのように長いものもあり、各パケット長は固定長でも可変長でも良い。ＭＰＥＧ２－ＰＳ（プログラム・ストリーム）では、映像、音声、補助データ等のデータの上位にパック・レイヤと称する階層があり、通常は複数個のパケットを束ねたパックと呼ばれる単位で取り扱われる。

【００４１】このようにして構成された多重ビットストリームのデータ構造は、ＭＰＥＧ２－ＰＳ（Ｐｒｏｇｒａｍ　Ｓｔｒｅａｍ）に準じていて、そのデータ構造とビットストリームは、以下のように階層的構造になっている。このビットストリームは、１ビットのフラグ等を多数有し、ヘッダ信号等の各セクター単位毎にバイト整列されたバイトストリームとなっていて、固定長でないデータ部分には、長さを示す情報が先行して置かれ、不要な部分をスキップしたりできる構成となっている。

【００４２】多重ビットストリームのデータ構造（ＭＰＥＧ２－ＰＳ）は、下位レイヤ（パケットレイヤ）と上位レイヤ（パックレイヤ）とを有する。上位レイヤ（パックレイヤ）については、以下のように構成される。１つのプログラムは、シーケンスと称されることもあり、先頭のパックヘッダに始まり、終了コードで終わる。パックは、一般に複数個のパケットから構成され、プログラムの先頭のパックには、システムヘッダと称されるストリーム全体の概要をパラメータ情報として記述した情報グループがある。このシステムヘッダは、先頭のパックには、付加することが義務づけられているが、２番目以降のパックではオプションとなっている。

【００４３】下位レイヤ（パケットレイヤ）については、以下のように構成される。ＭＰＥＧのパケットはＰＥＳ（Ｐｅｃｋｅｉｚｅｄ　Ｅｌｅｍｎｔａｒｙ　ＳｔｒｅｍＰａｃｋｅｔ）と称され、この構造は、ＭＰＥＧ２－ＴＳと共用して用いられるため、ヘッダ部分が複雑になっているが、階層的に理解し易くなっている。３２ビットの「パケット開始コード」は、２４ビットの固定部分と８ビットのストリームＩＤ（識別）部分からなる。ＭＰＥＧ２－ＰＳでは、最大でビデオ１６チャンネル、オーディオ３２チャンネルまで可能となるようにストリームＩＤが定義されている。これに続く「パケット長」は、このフィールドに続くパケットのデータ長を示す。パケット長に続く２ビットの制御コードはＭＰＥＧ１との識別用に用いられている。

【００４４】このようにして、生成されたオーサリングデータは信号データおよびキー信号出力回路に供給されて、ディスク出力部、テープ出力部、ハードディスク出力部またはオンラインデータ出力部のうちから選択された出力部において該当する記録媒体に記録される。このような信号データおよびキー信号出力回路から出力されて各記録媒体に記録されるデータを完パケデータと呼んでいる。

【００４５】次に、図３において、ディスクカッティング工場のフォーマッタ部の詳細構成を説明する。また、マスターキー１は、エージェント４で独自に生成され、具体的には、５バイトの２進数で、８ビットでマッピングされていて、それを用いてエンクリプトしたエンクリプトマスターキー２と生のマスターキー２等をエージェント４が供給し、マスターキー２検出部２２は、エージェント４からこれらキー信号関連信号を供給してもらい、それら各種関連キー信号群からデータ信号スクランブル用の生のマスターキーを得る。

【００４６】通常のＣＭＳではデータをスクランブルするタイトルキー、タイトルキーをエンクリプトする（マスター）ディスクキー（＝マスターキー２）、例えばパソコン（ＰＣ）間でデータのやりとりを行うための照合用のオーセンティックコントロール（ＡＣ）コードがある。

【００４７】本実施の形態のＣＭＳシステム関連信号は、（マスター）ディスクキーとしてエージェント４からマスターキー２／その他ＣＭＳシステム関連信号検出部２１へ供給される。タイトルキー（キー信号）はフォーマッタ部のキー信号生成部２４において生成される。そして、マスターキー２検出部２２において生のマスターキー２が検出され、キー信号エンクリプション部２５においてマスターキー２によりタイトルキー（キー信号）がエンクリプションされる。

【００４８】この場合、区間用乱数発生部３５においてスクランブルされるべき領域の圧縮ＡＶデータにスクランブルをかけると共にキー信号にエンクリプションをかける際のキー信号暗号化区間制御情報としての区間用乱数を発生させるようにし、スクランブル部２７においてスクランブルされるべき領域の圧縮ＡＶデータにキー信号暗号化区間制御情報に基づく区間にスクランブルをかけるようにし、キー信号エンクリプション部２５においてキー信号暗号化区間制御情報に基づく区間にエンクリプションをかけるようにする。

【００４９】つまり、キー信号用乱数発生部２３で発生させたキー信号に対してさらに区間用乱数発生部３５で指定された区間に、スクランブル部２７において元のデータ信号へのスクランブルを行ない、キー信号エンクリプション部２５においてキー信号のエンクリプションをかけるようにする。なお、スクランブルおよびエンクリプションをかける区間はセクター検出部３４で検出されたセクター区間により決めるようにする。また、区間用乱数発生部３５において特定の区間内の乱数を発生するようにしても良いし、または任意の区間毎の乱数を発生するようにしても良い。また、区間用乱数発生部３５において特定の区間内だけ乱数を発生しないようにしても良いし、または任意の区間毎だけ乱数を発生しないようにしても良い。

【００５０】より詳細には、キー信号エンクリプション部２５において、ディスクキーは、生のディスクキーデータをエージェント４が所有する２つで１組となっているマスターキー１（４０８組程度）を使って特定の区間でエンクリプトし、エンクリプトしたディスクキーとしてＣＭＳ関連信号／キー信号挿入部２８において被スクランブル信号に挿入される。そして、このエンクリプトしたディスクキー（＝マスターキー２）がディスクに記録されて外部に出ることになる。

【００５１】再生時には、ディスクプレイヤーにおいて、特定の区間でエンクリプトしたディスクキーはエージェント４により許可されて供給された１組のマスターキー１を持つＩＣ内部で、そのマスターキー１と照合され、所定の処理を経て使用された生のディスクキーとして取り出され、それによりタイトルキー（キー信号）を導き出し、データをディスクランブルする。

【００５２】つまり、再生側では、マスターキーを用いて特定の区間のエンクリプションを解いてキー信号に戻し、このキー信号を用いてディスクランブルをかけるようにする。この場合、ヘッダにあるエンクリプションをかけた区間を示すフラグを検出することにより、エンクリプションをかけた特定の区間を検出することができる。

【００５３】なお、上述した説明では、ディスクキーは以前述べているマスターキー２を現している。このように、スクランブルのためのキー信号はエージェント４から供給されるではなく、フォーマッタ内部で生成し、処理することで外部からうかがい知ることができないようにしている。また、さらにフォーマッタ内部で乱数を発生させてデータにスクランブルをかける区間長または時間を変化させると共に、キー信号の暗号化を複雑にすることにより、この暗号化を解くことを困難にしている。また、キー信号生成部２４において、生成されるキー信号は、例えば、５バイトの２進数であるが、キー信号のエンクリプションを行う区間や時間を変化させる場合は、８ビット程度の２進数である。

【００５４】また、キー信号エンクリプション部において、例えば、エンクリプションの方法は、そのキー信号の値からスクランブルの初期値とスクランブルの回数とを導いて、それから求めたり、マッピングにより特定の値を決めるようにしている。また、ＣＭＳ関連信号／キー信号挿入部２８において外部から読み取られないようにエンクリプションされたキー信号およびキー信号暗号化制御情報は、例えば、ＤＶＤでは被スクランブル信号のデータの前のリードイン部分、および各データパケットのヘッダ部分に挿入される。

【００５５】被スクランブル領域分離部２６は、同期検出回路と、信号分離回路とを有する。同期検出回路は、ヘッダ信号を検出し、ヘッダ信号に含まれる同期信号を検出する構成を有する。信号分離回路はこの同期信号に基づいてスクランブルされるべき信号領域を分離する。

ビットストリームからヘッダを検出する処理を以下に示す。ＭＰＥＧ２のビデオデータのデータ構造は、シーケンス層、ＧＯＰ層、ピクチャ層、スライス層、マクロブロック（ＭＢ）層、ブロック層の６層階層を有している。画像タイプに関して、ピクチャにはＩピクチャ、（フレーム内符号化画像）、Ｐピクチャ（フレーム間順方向予測符号化画像）、Ｂピクチャ（双方向予測符号化画像）の３種類があり、これらは、ピクチャ層のヘッダ中のＰＳＣ（Ｐｉｃｔｕｒｅ　Ｃｏｄｉｎｇ　Ｔｙｐｅ）によって特定することができる。

【００５６】また、オーディオビットストリームからヘッダを検出する処理を以下に示す。ＭＰＥＧオーディオの構造は、ＭＰＥＧオーディオのビットストリームの１フレームをＡＡＵ（Ａｕｄｉｏ　Ａｃｃｅｓｓ　Ｕｎｉｔ）と呼び、このＡＡＵのヘッダの同期ワードを検出することにより、オーディオデータのヘッダを検出することができる。

【００５７】同期検出の処理を以下に示す。同期検出は、アクセスユニット単位で行われる。例えば、映像信号では１フレーム、音声信号では１オーディオフレームがアクセスユニットとなる。ＭＰＥＧ２の同期方式は、映像信号、音声信号、補助データ信号等の他のデータの各アクセスユニットに、いつ同期検出、再生復号すべきかを示すタイムスタンプという情報が付加されている。このタイムスタンプには、ＳＣＲ（Ｓｙｓｔｅｍ　Ｃｌｏｃｋ　Ｒｅｆｅｒｅｎｃｅ、システム時刻基準参照値）という情報によって時間基準が与えられる。このタイムスタンプには、ＰＴＳ（再生出力の時刻管理情報）とＤＴＳ（復号の時刻管理情報）の２つがある。

【００５８】また、被スクランブル領域分離部２６は、ビットストリームから映像信号、音声信号、補助データ信号をそれぞれ個別のビットストリームに分離するように構成される。被スクランブル領域分離部２６は、ディマルチプレクス回路であり、マルチプレクス回路と逆の動作を行う回路である。

【００５９】この誤り訂正コードは、リードソロモン積符号をインターリーブで結合した形式で、ＣＩＲＣ（Ｃｒｏｓｓ　Ｉｎｔｅｒｌｅａｖｅｄ　Ｒｅｅｄ　Ｓｏｌｏｍｏｎ　Ｃｏｄｅ）を用いている。

【００６０】セクタ検出部３４は、ヘッダ信号が挿入された信号ブロック単位、つまり、セクター単位で各信号を生成するように構成される。このセクター検出部３４により検出されたセクターに基づいて区間用乱数発生部３５においてデータのスクランブルおよびキー信号のエンクリプションを行う区間の情報を発生させる。

【００６１】ディスクカッティング用信号処理部３０の８／１６変調回路は、元の信号を８ビット毎に区切り、記録信号を１６ビットに対応させるＥＦＭｐｌｕｓ変調を行うように構成される。また、カッティング部のレーザ変調器３１は、カッティング用ガスレーザ光をデータ信号に従って変調させる。カッティング用レーザービーム部３２は、変調されたレーザビームと、マスターディスクとを有する。レーザビームは、ガスレーザで出力され前述の変調器で変調される。マスターディスクは、ＤＶＤの製版の原盤となるディスクである。図示はしないが、マスターディスクは、カッティング中にはステッピングモーター等の回転駆動手段により回転駆動される構成となっている。

【００６２】このように構成された本実施の形態のディスクカッティング工場のフォーマッタ部とカッティング部は、以下のような動作をする。まず、ディスクカッティング工場の前段のオーサリングスタジオによれば以下のような動作をする。図２に示すオーサリングスタジオ２において、著作権者１のＡＶデータを入力する信号データ入力部からオリジナルの信号データがエンコードおよびマルチプレクス回路に供給される。具体的には、映像信号入力部からエンコード回路に映像信号が供給され、音声信号入力部からエンコード回路に音声信号が供給され、補助データ信号入力部からエンコード回路に補助データ信号がそれぞれ供給される。エンコード回路において映像信号はＭＰＥＧ２標準による動画圧縮符号化を施される。エンコード回路において音声信号はＭＰＥＧ２標準によるオーディオ符号化を施される。エンコード回路において補助データ信号は所定の符号化を施される。各エンコード回路において符号化された信号はマルチプレクス回路に供給される。マルチプレクス回路において各信号は、映像、音声、補助データ等のデータのパケットに切り換えられて、時分割して多重化され一本のビットストリームに変換される。

【００６３】図３に示すディスクカッティング工場において、上述した記録媒体に記録されて出力された完パケデータが被スクランブル領域分離部２６の同期検出回路に供給される。同期検出回路において、同期信号が検出され、検出された同期信号に基づいてデータ信号部が抽出される。

【００６４】また、同期検出されたビットストリームはスクランブルすべき信号領域の分離回路に供給される。信号分離回路において、多重化されたビットストリームから映像信号、音声信号、補助データ信号のそれぞれ個別のビットストリームが分離される。分離された映像信号、音声信号、補助データ信号のそれぞれ個別のビットストリームはスクランブル部２７に供給される。

【００６５】エージェント４においてフォーマット部内部で生成するキー信号をエンクリプションするマスターキー２とその他ＣＭＳシステム関連信号が生成され、フォーマッタ部のマスターキー２／その他ＣＭＳシステム関連信号検出部２１に供給される。マスターキー２／その他ＣＭＳシステム関連信号検出部２１において、エージェント４から供給されるキー信号関連信号からフォーマット部内部で生成するキー信号をエンクリプションす

るためのマスターキー２が検出される。マスターキー２はマスターキー２検出部２２に供給される。マスターキー２検出部２２において、マスターキー２が検出される。

【００６６】また、キー信号用乱数発生部２３において乱数が発生される。乱数はキー信号生成部２４に供給される。キー信号生成部２４において、キー信号用乱数および区間用乱数に基づいて区間が制御されたキー信号が生成される。キー信号はキー信号エンクリプション部２５およびスクランブル部２７に供給される。また、セクター検出部３４でセクター単位が検出され、セクター単位は区間用乱数発生部３５に供給される。区間用乱数発生部３５において、データのスクランブルおよびキー信号のエンクリプションに用いるキー信号暗号化区間制御情報が発生される。キー信号はキー信号生成部２４およびスクランブル部２７に供給される。スクランブル部２７において、スクランブルされるべき領域の圧縮ＡＶデータに対してフォーマッタ部内部でキー信号用乱数および区間用乱数に基づいて区間が制御されて生成されたキー信号によりスクランブルが行われる。

【００６７】また、キー信号エンクリプション部２５において、フォーマッタ部内部で乱数に基づいて区間が制御されて生成されたキー信号がマスターキー２によりエンクリプションされる。エンクリプションされたキー信号、キー信号暗号化区間制御情報およびスクランブルされた被スクランブル信号がＣＭＳ関連信号／キー信号挿入部２８に供給される。また、マスターキー２／その他ＣＭＳシステム関連信号検出部２１からＣＭＳ関連信号がＣＭＳ関連信号／キー信号挿入部２８に供給される。ＣＭＳ関連信号／キー信号挿入部２８において、スクランブルされた圧縮ＡＶデータにエンクリプションされたキー信号、キー信号暗号化区間制御情報およびその他ＣＭＳシステム関連信号が挿入される。

【００６８】エンクリプションされたキー信号が挿入されたスクランブルされた圧縮ＡＶデータは誤り検出／誤り訂正コード付加部２９に供給される。誤り検出／誤り訂正コード付加部２９において、データに誤り検出コード（ＥＤＣ）が付加され、誤り訂正コード（ＥＣＣ）処理が施される。誤り検出／誤り訂正コード付加されたデータはディスクカッティング用信号処理部３０に供給される。ディスクカッティング用信号処理部３０において、ディスクに記録する信号に適した８／１６変調や、付加情報を含む同期信号を信号ブロックの先頭に挿入する同期挿入等の処理が施される。ディスクカッティング用信号処理されたデータはレーザ変調器３１に供給される。

【００６９】レーザ変調器３１において、８／１６変調や同期挿入等の処理を施したデータに従って変調器で変調が施される。カッティング用レーザービーム部３２において、レーザビームはこの変調器３１でレーザ変調され、それによりマスターディスクをカッティングしてコピーガード付マスターディスク３３が作成される。

【００７０】ここで、上述したように、マスターキー１は、エージェント４で独自に生成され、具体的には、５バイトの２進数で、８ビットでマッピングされていて、これを用いてマスターキー２をエンクリプトする。マスターキー２検出部２２において、エージェント４から供給された各種キー信号群から、生のマスターキー２を得る。

【００７１】本実施の形態のＣＭＳシステム関連信号は、特に、（マスター）ディスクキー（＝マスターキー２）がエージェント４からマスターキー２／その他ＣＭＳシステム関連信号検出部２１へ供給される。タイトルキー（キー信号）はフォーマッタ部のキー信号生成部２４において生成される。そして、マスターキー２検出部２２においてマスターキー２が検出され、キー信号エンクリプション部２５においてマスターキー２によりタイトルキー（キー信号）がエンクリプションされる。

【００７２】この場合、区間用乱数発生部３５においてデータにスクランブルをかけると共にキー信号にエンクリプションをかける際のキー信号暗号化区間制御情報としての区間用乱数を発生させるようにし、スクランブル部２７においてキー信号暗号化区間制御情報に基づく区間にスクランブルをかけ、キー信号エンクリプション部２５においてキー信号暗号化区間制御情報に基づく区間にエンクリプションをかけるようにする。

【００７３】つまり、キー信号用乱数発生部２３で発生させたキー信号に対してさらに区間用乱数発生部３５で指定された区間に、スクランブル部２７においてデータのスクランブルをかけると共に、キー信号エンクリプション部２５においてキー信号のエンクリプションをかけるようにする。なお、スクランブルおよびエンクリプションをかける区間はセクター検出部３４で検出されたセクター区間により決めるようにする。また、区間用乱数発生部３５において特定の区間内の乱数を発生するようにしても良いし、または任意の区間毎の乱数を発生するようにしても良い。また、区間用乱数発生部３５において特定の区間内だけ乱数を発生しないようにしても良いし、または任意の区間毎だけ乱数を発生しないようにしても良い。

【００７４】より詳細には、キー信号エンクリプション部２５において、ディスクキーが、エージェント４が所有するマスターキー１を使ってエンクリプトされ、エンクリプトされたディスクキーとしてＣＭＳ関連信号／キー信号挿入部２８において被スクランブル信号に挿入される。そして、このエンクリプトされたディスクキーがディスクに記録されて外部に出される。

【００７５】再生時には、ディスクプレイヤーにおいて、エンクリプトされたディスクキーはエージェント４により許可されて供給された１組のマスターキー１をも

つＩＣ内部で、そのマスターキー１と照合され、ディスクリプションされて生のディスクキーとして取り出され、それにより同じくディスクリプションすることによりタイトルキー（キー信号）が導き出され、同様にディスクリプションをほどこしてデータがディスクランブルされる。

【００７６】つまり、再生側では、マスターキー１とディスクキーを用いて特定の区間のエンクリプションを解いてキー信号に戻し、このキー信号を用いてディスクランブルをかけるようにする。この場合、ヘッダにあるエンクリプションをかけた区間を示すフラグを検出することにより、エンクリプションをかけた特定の区間を検出することができる。

【００７７】また、キー信号エンクリプション部２５において、例えば、そのキー信号の値からスクランブルの初期値とスクランブルの回数とが導かれて、それから求めた値によりエンクリプションが行われたり、マッピングにより特定の値を決めることにより、エンクリプションが行われるようにしている。

【００７８】また、ＣＭＳ関連信号／キー信号挿入部２８において外部から読み取られないようにエンクリプションされたキー信号は、例えば、ＤＶＤでは被スクランブル信号のデータの前のリードイン部分、および各データパケットのヘッダ部分に挿入される。

【００７９】また、ディスクカッティング用信号処理部３０の８／１６変調回路において、元の信号は８ビット毎に区切られ、記録信号を１６ビットに対応させるＥＦＭｐｌｕｓ変調が行われる。８／１６変調された信号はカッティング部のレーザ変調器３１に供給される。レーザ変調器３１において、８／１６変調された信号に基づいてレーザビームが変調される。カッティング用レーザビーム部３２において、マスターディスクに前述の変調器によりビームが変調されたレーザビームのレーザ光を照射してカッティングを行い、ＤＶＤの製版の原盤となるコピーガード付きマスターディスク３３が作成される。このようにして作られたマスターディスクを用いてスタンピングすることにより商用のディスクを多数作成することができる。

【００８０】このように、本実施の形態では、キー信号をエンクリプションするマスターキー２とそのマスターキー２によりキー信号のエンクリプション処理を実行するキー信号エンクリプション部２５をディスクカッティング工場のフォーマッタ部に予め設けておき、かつ同時にフォーマッタ部に設けられたキー信号用乱数発生部２３によりキー信号を生成するようにすると共に、区間用乱数発生部３５により元のデータ信号にスクランブルをかけると共にキー信号をエンクリプションする区間を制御するようにした。このようにして生じさせたキー信号によりディスクカッティング工場のフォーマッタ部内部で、入力されたデータ列に特定区間でスクランブルをかけ、そのキー信号にマスターキー２を用いて特定区間にキー信号エンクリプション部２５によりエンクリプションをかけ、このキー信号と区間制御情報とを所定のデータ信号部分に挿入し、その暗号化されたデータ列をその他の後段の信号処理を経て、マスターディスクカッティング用信号として出力するようにした。

【００８１】なお、ここでは、元のデータにスクランブルをかけると共にキー信号の暗号化のためにエンクリプションを行うセクター区間を、フォーマッタに内蔵されている区間用乱数発生部３５で発生する乱数で制御し、元のデータ列のうちのどのセクター部分がエンクリプト処理されているかが外部の第三者が容易に分からないようにするものである。もちろんエンクリプト処理の有無は、各セクター毎に分かるようにヘッダー部分のエンクリプトされたキー信号の有無またはヘッダー部分にあるフラグによりどのセクターの信号部分にエンクリプションがかけられているかを区別することができる。なお、ここで、キー信号用乱数発生部２３やキー信号エンクリプション部２５は、ハードウエアにより構成することもできるが、ソフトウエアにより構成するようにしてもよい。

【００８２】このように、キー信号はエージェント４から供給されるではなく、フォーマッタ内部で生成し、処理することで外部からうかがい知ることができないようにしている。また、さらにフォーマッタ内部で乱数を発生させてデータにスクランブルをかける区間長または時間を変化させることにより、キー信号の暗号化を複雑にしてこの暗号化を解くことを困難にしている。

【００８３】また、この場合、元のデータ列が入力され、ＣＭＳで処理され、マスターディスクカッティング用信号として出力されてディスクとなる間に、キー信号はフォーマッタの外部には一度もでることがなく、外部からはどのような値であるかはうかがい知ることはできないようになっている。また、その場合のエンクリプション処理されたキー信号のセクターがどの位置にまたはどのような頻度で現れるかも分からなくなり、たとえ、キー信号が盗まれてもデータの不正コピーのためには各セクターをエンクリプションされているかどうか逐次チェックし、必要なセクターのみのエンクリプションを解いていくことが要求されるのでデータの不正コピーが困難となる。

【００８４】このように、本実施の形態のＣＭＳでは、元のデータ列にスクランブルをかけることで、出力データからは一義的に元のデータ列を再現できないようにしているが、再生側で、スクランブルをかけたキー信号がわかれば比較的容易にそのキー信号でディスクランブルして、元のデータ列を再生することができるが、このようにキー信号のエンクリプションがかかっているセクター区間が変化するので元のデータ列の再生は容易ではない。

【００８５】以上述べたように、本実施の形態では、元のデータ列にスクランブルをかけているキー信号をフォーマッタの外部に出さないようにすると共に、キー信号にエンクリプションをかける区間を制御して一切外部に出さないようにすることにより、キー信号の暗号化を複雑にし、第三者がこのキー信号を知ってディスクランブルをかけることが一層困難になるので、不正なコピーを防止することができる。

【００８６】また、上述した本実施の形態によれば、各セクターのうちのエンクリプションを行うセクター区間を乱数により制御するようにしたが、逆に一律に各セクターにエンクリプションをかけたうちで、乱数によりエンクリプション処理を停止する区間を制御して、同様に、元のデータ列のうちのどのセクター部分がエンクリプション処理されているかをいないかを分からないようにするようにしても良い。このようにすることにより、上述と同様の不正コピー防止の効果が得られる。もちろんこの場合もエンクリプション処理の有無は、各セクター毎に分かるようにヘッダー部分のエンクリプションされたキー信号の有無またはヘッダー部分のフラグでエンクリプションされた区間を区別することができる。

【００８７】また、このようなことから派生して、エンクリプション処理を行う区間を制御する乱数でキー信号に関わる乱数をコントロールする、つまり、区間の乱数で指定されるタイミングで、キー信号に関わる乱数によりキー信号の数値を変化させるようにしても良い。このように、元のデータ列にスクランブルをかけるキー信号を、時間間隔的にも、内容的にも、フォーマッタ内部でクローズドで変化させることにより、外部からのキー信号の盗用は極めて困難になり、不正コピーに対する強力な防止対策を実現させることができる。

【００８８】この実施の形態の記録媒体としてのディスクは、複数の素材信号がそれぞれ符号化され、符号化された複数の素材信号が多重化されてオリジナル信号が新規に作成されたとき、上記オリジナル信号が所定のキー信号に基づいてスクランブルされた被スクランブル信号と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号と、特定の区間または任意の区間毎に上記オリジナル信号のスクランブルおよび上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報と、を記録するようにしたので、キー信号の暗号化の区間を制御して、キー信号の暗号化を複雑にすることにより、第三者は記録媒体としてのディスクから直接キー信号を得ることができず、キー信号の受け渡し時に生じ易いキー信号の盗用を防止することができ、これにより、第三者による記録媒体としてのディスクの素材信号の不正コピーを防止することができる。

【００８９】また、この実施の形態のディスクカッティング装置は、入力信号から、上記入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成するキー信号生成手段としてのキー信号用乱数発生部２３と、上記キー信号に基づいて上記入力信号に対してスクランブルをかけるスクランブル手段としてのスクランブル部２７と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを、上記スクランブル手段としてのスクランブル部２７によりスクランブルをかけられた被スクランブル信号に挿入する挿入手段としてのＣＭＳ関連信号／キー信号挿入部２８と、を備え、上記挿入手段としてのＣＭＳ関連信号／キー信号挿入部２８により上記暗号化キー信号および上記暗号化区間制御情報とを上記被スクランブル信号に挿入したデータからカッティングデータを生成して、上記カッティングデータに基づいてマスターディスクを作成するようにしたので、キー信号とそのキー信号の動作する区間制御情報を装置内部で自動生成して人間等の介在を取り除き、ディスクカッティング工程において、外部にキー信号が出ることがなく、しかも、キー信号の暗号化を複雑にするので、キー信号の機密性を高めることができ、第三者は記録媒体から直接キー信号を得ることができず、キー信号の受け渡し時に生じ易いキー信号の盗用を防止することができ、これにより、第三者による記録媒体の素材信号の不正コピーを防止することができる。

【００９０】

【発明の効果】この発明の記録媒体は、複数の素材信号がそれぞれ符号化され、符号化された複数の素材信号が多重化されてオリジナル信号が新規に作成されたとき、上記オリジナル信号が所定のキー信号に基づいてスクランブルされた被スクランブル信号と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号と、特定の区間または任意の区間毎に上記オリジナル信号のスクランブルおよび上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報と、を記録するようにしたので、キー信号の暗号化の区間を制御して、キー信号の暗号化を複雑にすることにより、第三者は記録媒体から直接キー信号を得ることができず、キー信号の受け渡し時に生じ易いキー信号の盗用を防止することができ、これにより、第三者による記録媒体の素材信号の不正コピーを防止することができるという効果を奏する。

【００９１】また、この発明のディスクカッティング装置は、入力信号から、上記入力信号に対してスクランブルをかけるキー信号を乱数に基づいて生成するキー信号生成手段と、上記キー信号に基づいて上記入力信号に対してスクランブルをかけるスクランブル手段と、乱数に基づいて発生させた上記キー信号をさらに暗号化した暗号化キー信号および特定の区間または任意の区間毎に上記入力信号のスクランブルと上記キー信号の暗号化を行う区間を制御する暗号化区間制御情報とを、上記スクラ

ンブル手段によりスクランブルをかけられた被スクランブル信号に挿入する挿入手段と、を備え、上記挿入手段により上記暗号化キー信号および上記暗号化区間制御情報とを上記被スクランブル信号に挿入したデータからカッティングデータを生成して、上記カッティングデータに基づいてマスターディスクを作成するようにしたので、キー信号とそのキー信号の動作する区間制御情報を装置内部で自動生成して人間等の介在を取り除き、ディスクカッティング工程において、外部にキー信号が出ることがなく、しかも、キー信号の暗号化を複雑にするので、キー信号の機密性を高めることができ、第三者は記録媒体から直接キー信号を得ることができず、キー信号の受け渡し時に生じ易いキー信号の盗用を防止することができ、これにより、第三者による記録媒体の素材信号の不正コピーを防止するできるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の実施の形態のＣＭＳにおけるコピー防止システムの概要を示す図である。

【図２】本発明の実施の形態のディスクカッティング工場のフォーマッタ部の構成を示すブロック図である。

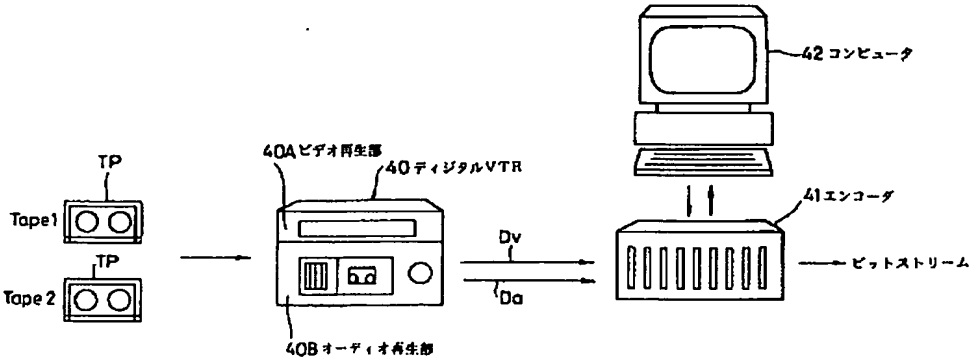
【図３】本発明の実施の形態のディスクカッティング工場のフォーマッタ部とカッティング部の構成を示すブロック図である。

【図４】従来のオーサリングシステムの構成を示す図である。

【符号の説明】

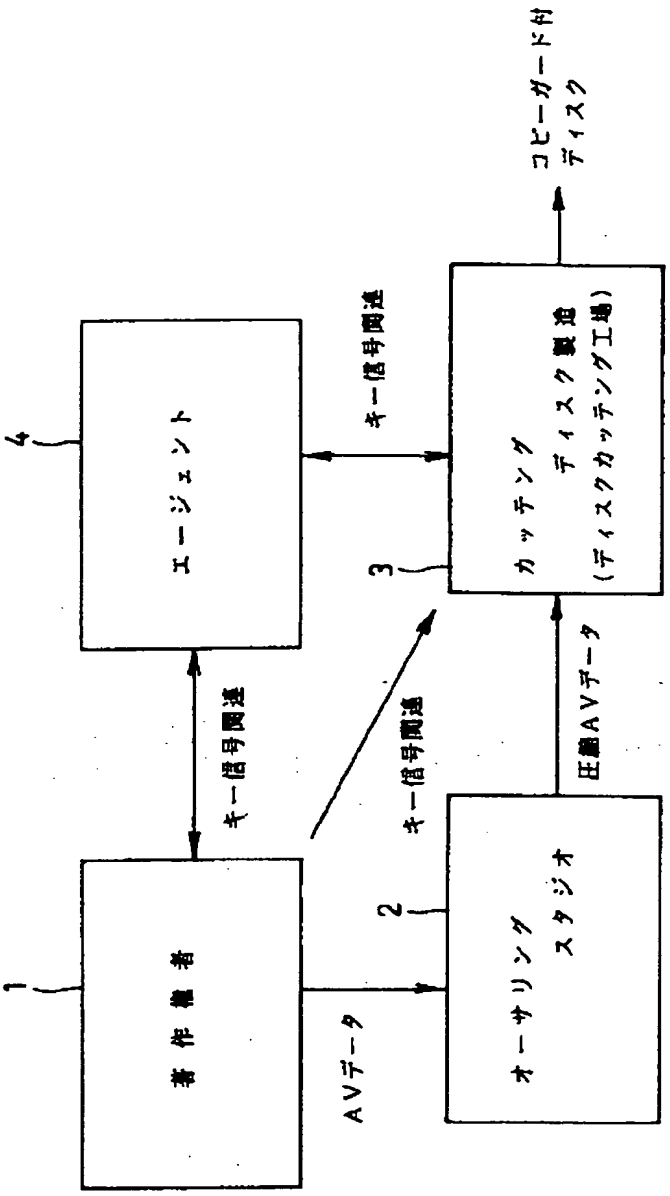
１　著作権者、２　オーサリングスタジオ、３　カッティングディスク製造（ディスクカッティング工場）、４　エージェント、１０　ディスクカッティング工場フォーマッタ部、１１　キー信号によるスクランブル部、１２　エンクリプテドキー信号挿入部、１３　フォーマッタによる信号変換部、２０　ディスクカッティング工場フォーマッタ部／カッティング部、２１　マスターキー２／その他ＣＭＳシステム関連信号検出部、２２　マスターキー２検出部、２３　キー信号用乱数発生部、２４　キー信号生成部、２５　キー信号エンクリプション部、２６　被スクランブル領域分離部、２７　スクランブル部、２８　ＣＭＳ関連信号／キー信号挿入部、２９　誤り検出／誤り訂正コード付加部、３０　ディスクカッティング用信号処理部、３１　レーザ変調部、３２　カッティング用レーザビーム部、３３　コピーガード付マスターディスク、３４　セクタ検出部、３５区間用乱数発生部

【図４】



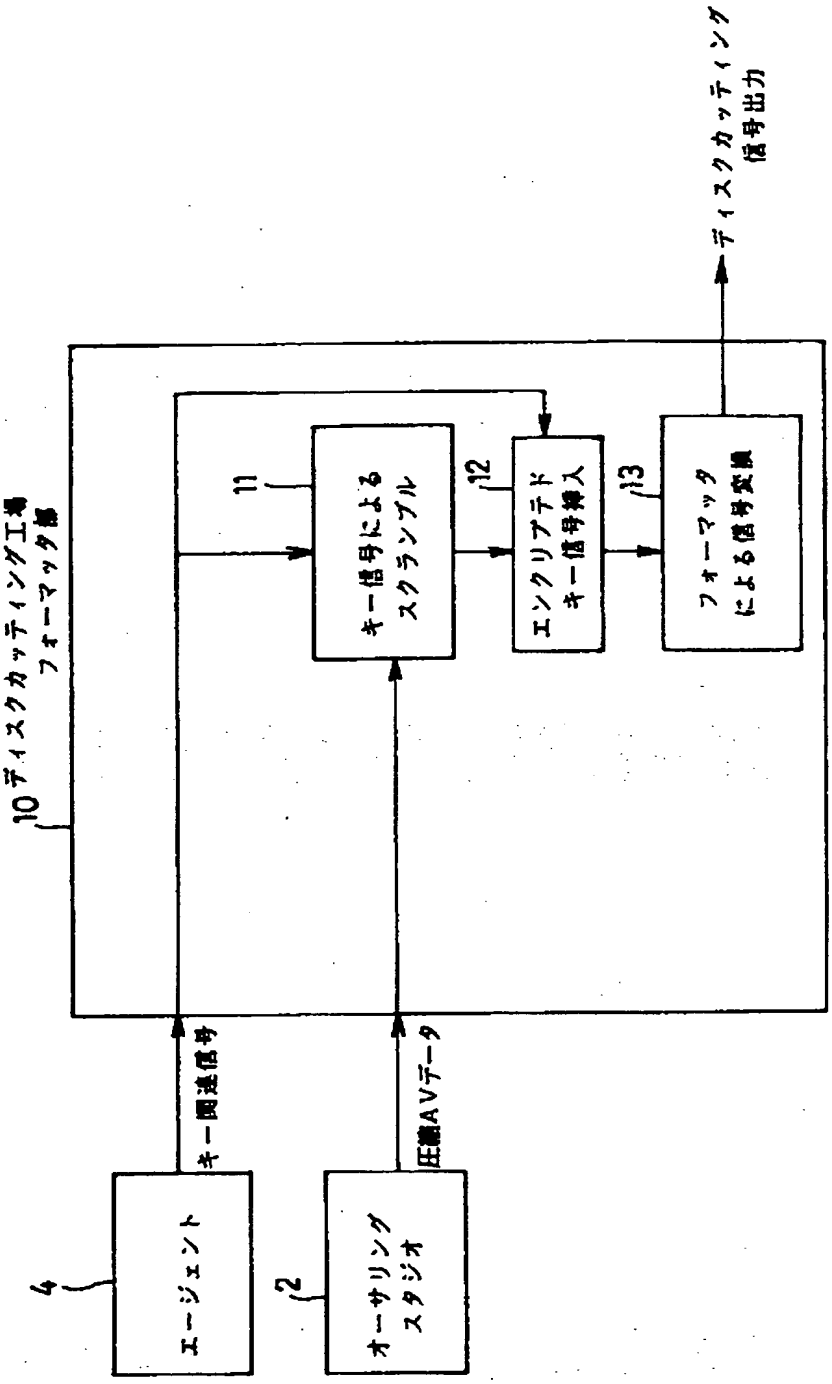
従来のオーサリングシステムの構成例

【図１】



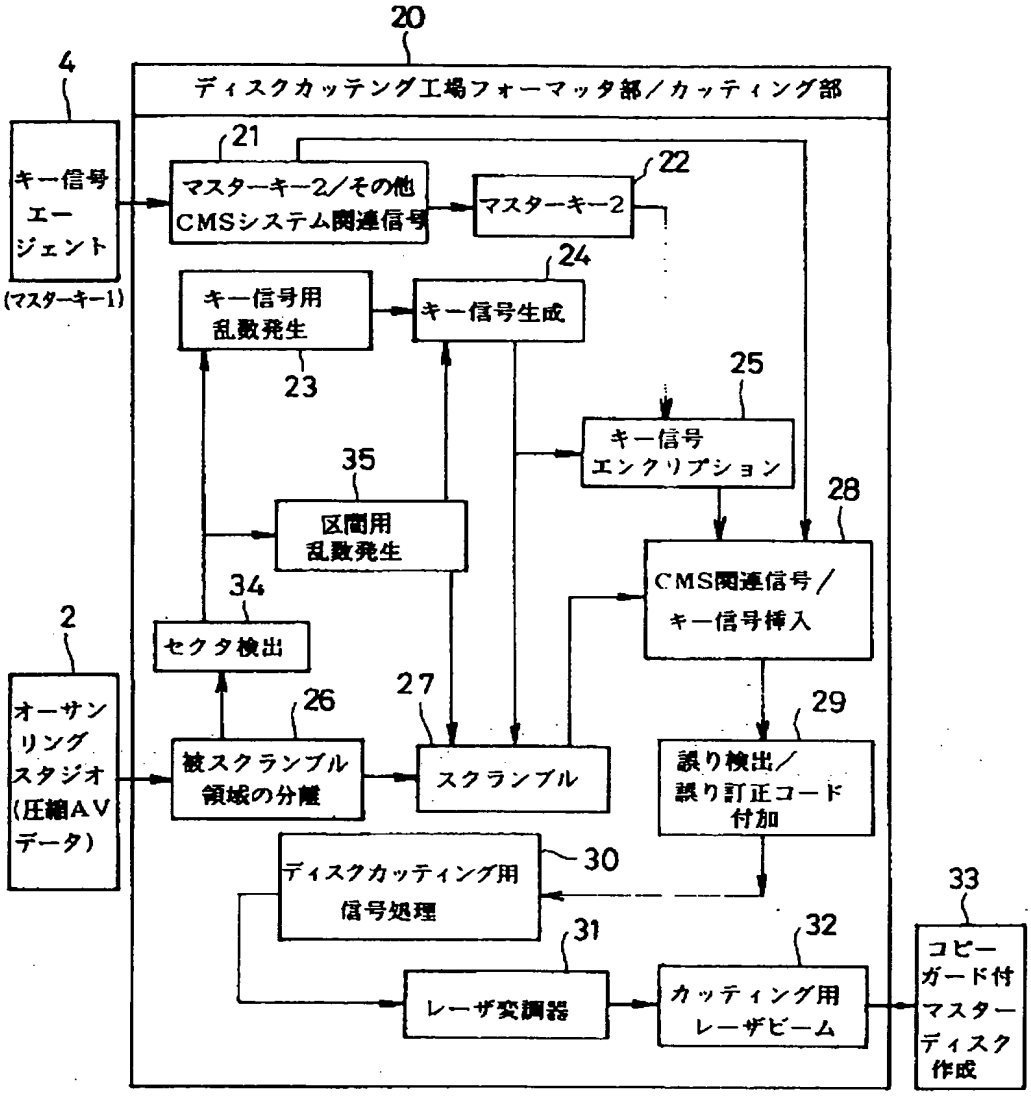
本実施の形態のCMSにおけるコピー防止システムの概要を示す図

【図２】



本実施の形態のディスクカッティング工場のフォーマッタ部の構成を示す図

【図３】



本実施の形態のディスクカッティング工場のフォーマッタ部とカッティング部の構成を示す図